AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A method for running a tamper-resistant application in a trusted environment, comprising:

defining a trusted virtual machine environment that contains a trusted dictionary for protecting data, wherein the trusted dictionary comprises a subclass of a standard base class dictionary using any class that allows a storing and a retrieving of data values, wherein the trusted dictionary contains keywords and values encrypted with a secret including a key, and wherein the trusted dictionary includes a list of public keys;

verifying the integrity of the application;

wherein, if the application is tampered with, the trusted virtual machine environment prevents the application from accessing the secret ~~secrets~~ in the trusted dictionary, thus disabling the normal operation of the application.

2. (Currently Amended) The method of claim 1, wherein if the integrity of the application is confirmed, the trusted virtual machine environment allows the application to access the secret ~~secrets~~ in the trusted dictionary, thus enabling the normal operation of the application.

3. (Original) The method of claim 2, wherein defining the trusted virtual machine environment comprises defining a trusted bundle for protecting a programming code of the application.

4. (Original) The method of claim 3, wherein protecting the programming

code comprises encrypting the programming code.

5. (Original) The method of claim 4, wherein the trusted virtual machine environment decrypts the encrypted programming code using a decryption key from a media key block associated with the application.

6. (Original) The method of claim 1, wherein defining the trusted virtual machine environment comprises using a security chip.

7. (Original) The method of claim 3, wherein defining the trusted bundle comprises restricting access to instruction codes of the trusted bundle.

8. (Original) The method of claim 1, further comprising encrypting the trusted dictionary.

9. (Original) The method of claim 1, wherein defining the trusted virtual machine environment comprises defining at least two trusted bundles; and

wherein the trusted dictionary is shared between at least some of the at least two trusted bundles, to maintain communication integrity between the at least two trusted bundles.

10. (Original) The method of claim 1, wherein the application comprises a player that plays copy-protected media.

11. (Original) The method of claim 10, wherein the trusted dictionary contains one or more decryption keys to decrypt the copy-protected media.

12-20 (Withdrawn)

21. (Currently Amended) A computer program product having instruction codes for running a tamper-resistant application in a trusted environment, comprising:

a first set of instruction codes for defining a trusted virtual machine environment that contains a trusted dictionary for protecting data, wherein the trusted dictionary comprises a subclass of a standard base class dictionary using any class that allows a storing and a retrieving of data values, wherein the trusted dictionary contains keywords and values encrypted with a secret including a key, and wherein the trusted dictionary includes a list of public keys;

a second set of instruction codes for verifying the integrity of the application;

wherein, if the application is tampered with, the trusted virtual machine environment prevents the application from accessing the secret ~~secrets~~ in the trusted dictionary, thus disabling the normal operation of the application.

22. (Currently Amended) The computer program product of claim 21, wherein if the integrity of the application is confirmed, the trusted virtual machine environment allows the application to access the secret ~~secrets~~ in the trusted dictionary, thus enabling the normal operation of the application.

23. (Original) The computer program product of claim 22, wherein the first set of instruction codes defines the trusted virtual machine environment by defining a trusted bundle for protecting a programming code of the application.

24. (Original) The computer program product of claim 23, wherein the first set of instruction codes protects the programming code by encrypting the programming code.

25. (Original) The computer program product of claim 24, wherein the trusted virtual machine environment decrypts the encrypted programming code using a decryption key from a media key block associated with the application.

26. (Original) The computer program product of claim 21, wherein the first set of instruction codes defines the trusted virtual machine environment comprises using a security chip.

27. (Original) The computer program product of claim 23, wherein the first set of instruction codes defines the trusted bundle by restricting access to the trusted bundle.

28. (Original) The computer program product of claim 21, further comprising a third set of instruction codes for encrypting the trusted dictionary.

29. (Original) The computer program product of claim 21, wherein the first set of instruction codes defines the trusted virtual machine environment by defining at least two trusted bundles; and

wherein the trusted dictionary is shared between at least some of the at least two trusted bundles, to maintain communication integrity between the at least two trusted bundles.

30. (Original) The computer program product of claim 21, wherein the application comprises a player that plays copy-protected media.

31. (Original) The computer program product of claim 30, wherein the trusted dictionary contains one or more decryption keys to decrypt the copy-protected media.

32.-40. (Withdrawn)

41. (Currently Amended) A ~~model~~ system for running a tamper-resistant application in a trusted environment, comprising:

a storage medium for storing a definition of a trusted virtual machine environment that contains a trusted dictionary for protecting data, wherein the trusted dictionary comprises a subclass of a standard base class dictionary using any class that allows a storing and a retrieving of data values, wherein the trusted dictionary contains keywords and values encrypted with a secret including a key, and wherein the trusted dictionary includes a list of public keys;

a server, operatively coupled to the storage medium, for performing a verification of the integrity of the application;

wherein, if the application is tampered with, the trusted virtual machine environment prevents the application from accessing secrets in the trusted dictionary, thus disabling the normal operation of the application.

42. (Currently Amended) The ~~model~~ system of claim 41, wherein if the integrity of the application is confirmed, the trusted virtual machine environment allows the application to access the secrets in the trusted dictionary, thus enabling the normal operation of the application.

43. (Currently Amended) The ~~model~~ system of claim 42, wherein the definition of the trusted virtual machine environment comprises a definition of a trusted bundle for protecting a programming code of the application.

44. (Currently Amended) The ~~model~~ system of claim 43, wherein the protection of the programming code comprises an encryption of the programming code.

45. (Currently Amended) The ~~model~~ system of claim 44, wherein the trusted virtual machine environment decrypts the encrypted programming code using a decryption key from a media key block associated with the application.

46. (Currently Amended) The ~~model~~ system of claim 41, wherein the definition of the trusted virtual machine environment comprises the use of a security chip.

47. (Currently Amended) The ~~model~~ system of claim 43, wherein the definition of the trusted bundle comprises a restriction of access to instruction codes of the trusted bundle.

48. (Currently Amended) The ~~model~~ system of claim 41, further comprising an encryption of the trusted dictionary.

49. (Currently Amended) The ~~model~~ system of claim 41, wherein the definition of the trusted virtual machine environment comprises a definition of at least two trusted bundles; and

wherein the trusted dictionary is shared between at least some of the at least two trusted bundles, to maintain communication integrity between the shared trusted dictionary.

50. (Currently Amended) The ~~model~~ system of claim 41, wherein the application comprises a player that plays copy-protected media.

51. (Currently Amended) The ~~model~~ system of claim 50, wherein the trusted dictionary contains one or more decryption keys to decrypt the copy-protected media.

52-60 (Withdrawn)